Datasäkerhet - Lab 1

Course DT523A

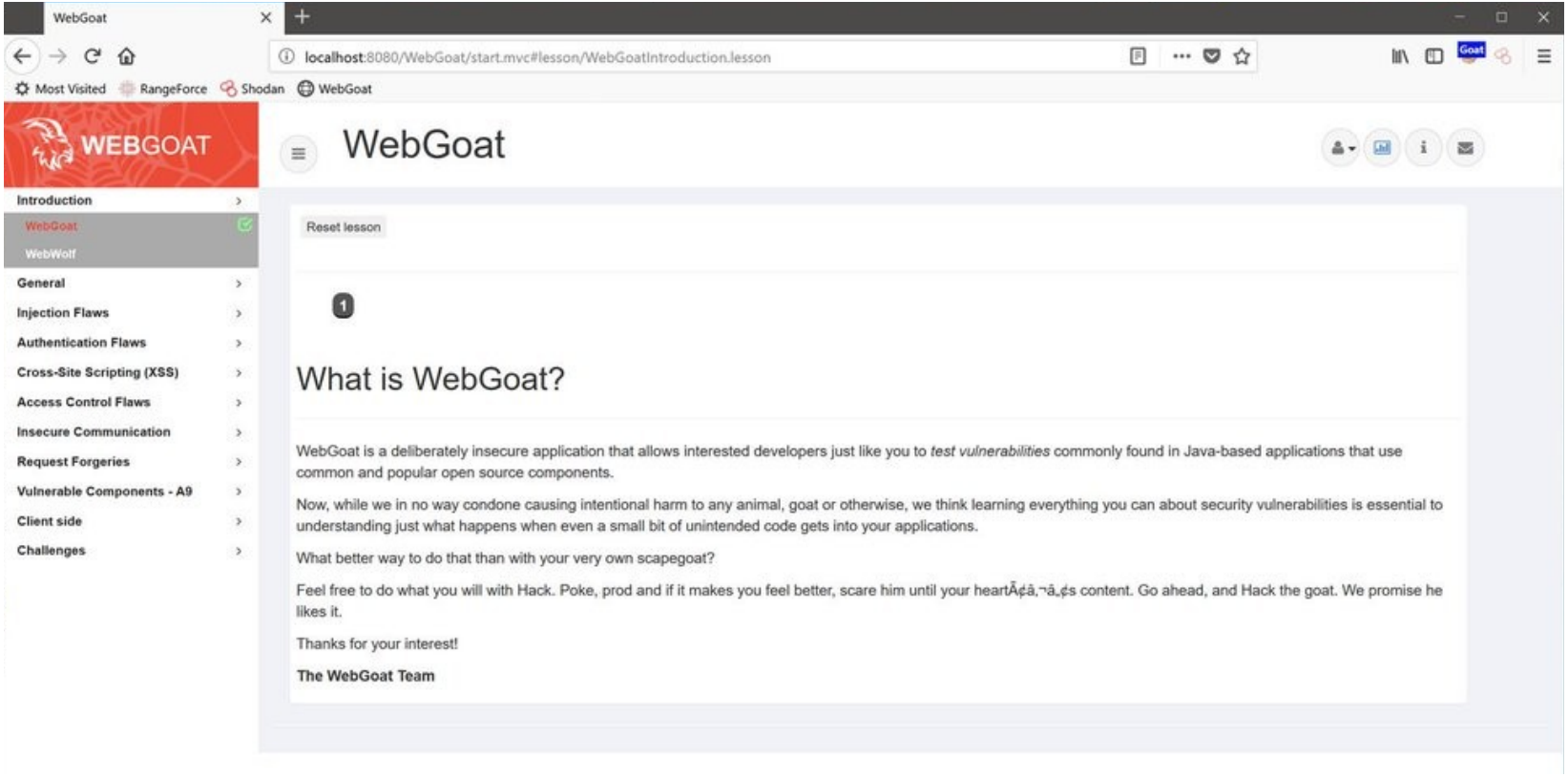
Alberto Giaretta, PhD
Centre for Applied Autonomous Sensor Systems (AASS)
Örebro University, Sweden

2022/2023

Broken Authentication

- To do the labs, you need 2 tools
  - OWASP WebGoat, a training webpage for basic hacking
  - OWASP ZAP, a HTTP attack proxy

OWASP WebGoat



OWASP WebGoat

- Comes as a docker image or a standalone jar file
- Jar: download it, open your OS terminal, move to the download folder and then execute
  - Download at:
    https://github.com/WebGoat/WebGoat/releases/download/v2023.4/webgoat-2023.4.jar
  - Execute as:
    java -jar webgoat-2023.4.jar --server.port 8080 –server.address=127.0.0.1

OWASP WebGoat

- Docker, on Ubuntu you install via
  - *snap install docker*
  - *sudo docker pull webgoat/webgoat*
  - *sudo docker run -p 127.0.0.1:8080:8080 -p 127.0.0.1:9090:9090 -e TZ=Europe/Amsterdam webgoat/webgoat*

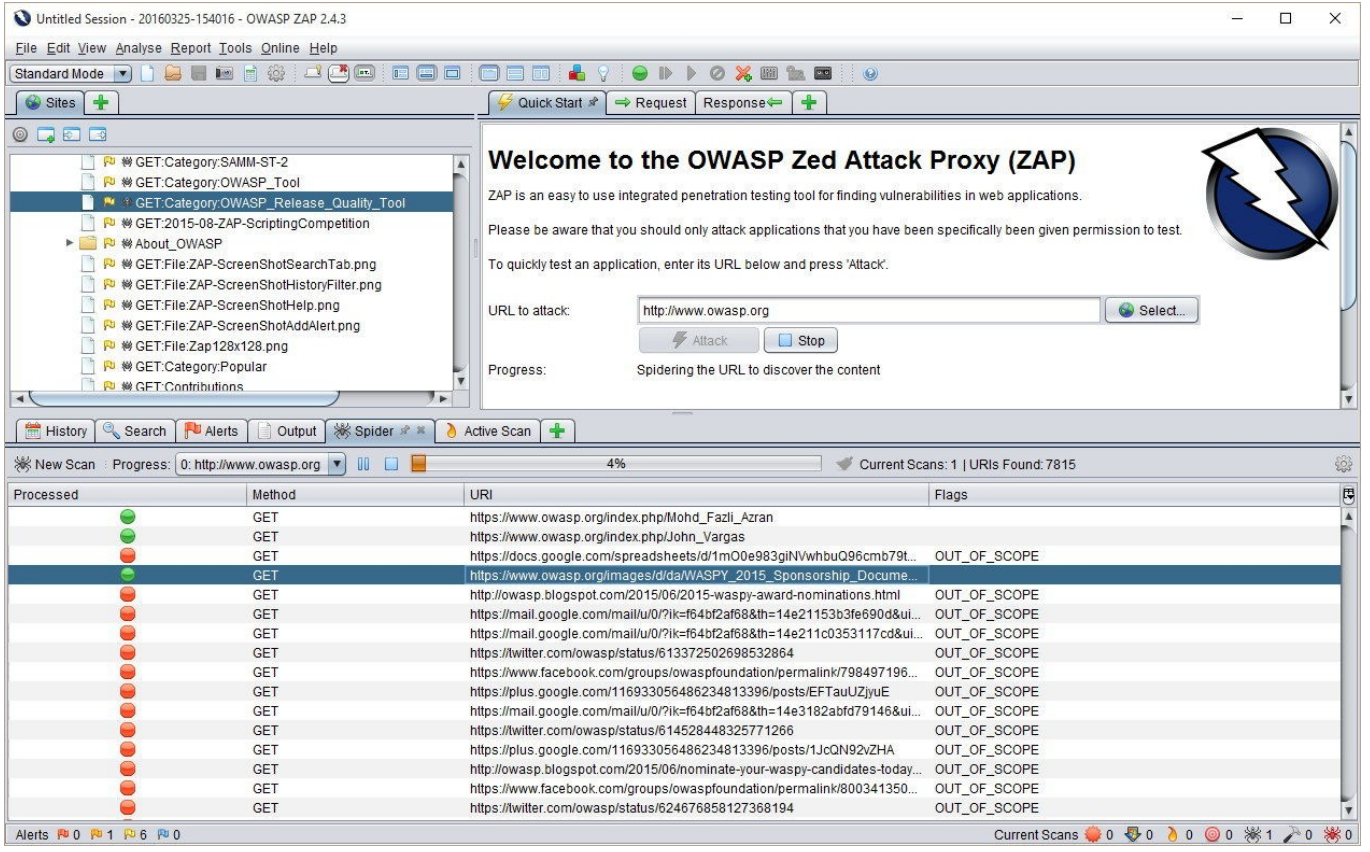
OWASP WebGoat

- Now you just go to http://127.0.0.1:8080/WebGoat
- You create an “account”
  - It’s a fake one, in your local pc, use whatever username/password combination you like
- You will see a lot of modules on the left
  - In the coming labs you will do some of them
- We will use this exercise webpage for other labs in the future, don’t throw it away!

OWASP ZAP

- This is a web app scanner
  - You can intercept the packages you send
  - You can verify the content of your packets and edit it, before forwarding
- Useful for changing the packets in a way that the websites would not allow!

OWASP ZAP


Untitled Session - 20160325-154016 - OWASP ZAP 2.4.3
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
GET:Category:SAMM-ST-2
GET:Category:OWASP_Tool
GET:Category:OWASP_Release_Quality_Tool
GET:2015-08-ZAP-ScriptingCompetition
About_OWASP
GET:File:ZAP-ScreenShotSearchTab.png
GET:File:ZAP-ScreenShotHistoryFilter.png
GET:File:ZAP-ScreenShotHelp.png
GET:File:ZAP-ScreenShotAddAlert.png
GET:File:Zap128x128.png
GET:Category:Popular
GET:Contributions
Welcome to the OWASP Zed Attack Proxy (ZAP)
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
To quickly test an application, enter its URL below and press 'Attack'.
URL to attack:
http://www.owasp.org
Select...
Attack
Stop
Progress:
Spidering the URL to discover the content
History
Search
Alerts
Output
Spider
Active Scan
New Scan
Progress:
0: http://www.owasp.org
4%
Current Scans: 1 | URIs Found: 7815
Processed
Method
URI
Flags
GET https://www.owasp.org/index.php/Mohd_Fazli_Azran
GET https://www.owasp.org/index.php/John_Vargas
GET https://docs.google.com/spreadsheets/d/1mO0e983giNVwhbuQ96cmb79t... OUT_OF_SCOPE
GET https://www.owasp.org/images/d/da/WASPY_2015_Sponsorship_Docume...
GET http://owasp.blogspot.com/2015/06/2015-waspy-award-nominations.html OUT_OF_SCOPE
GET https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e21153b3fe690d&ui... OUT_OF_SCOPE
GET https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e211c0353117cd&ui... OUT_OF_SCOPE
GET https://twitter.com/owasp/status/613372502698532864 OUT_OF_SCOPE
GET https://www.facebook.com/groups/owaspfoundation/permalink/798497196... OUT_OF_SCOPE
GET https://plus.google.com/116933056486234813396/posts/EFTauUZjyuE OUT_OF_SCOPE
GET https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e3182abfd79146&ui... OUT_OF_SCOPE
GET https://twitter.com/owasp/status/614528448325771266 OUT_OF_SCOPE
GET https://plus.google.com/116933056486234813396/posts/1JcQN92vZHA OUT_OF_SCOPE
GET http://owasp.blogspot.com/2015/06/nominate-your-waspy-candidates-today... OUT_OF_SCOPE
GET https://www.facebook.com/groups/owaspfoundation/permalink/800341350... OUT_OF_SCOPE
GET https://twitter.com/owasp/status/624676858127368194 OUT_OF_SCOPE
Alerts 0 1 6 0
Current Scans 0 0 0 0 1 0 0

OWASP ZAP

- You can download it here
  - *https://www.zaproxy.org/download/*
  - If you use Linux, there is also the snap

    sudo snap install zaproxy

Today Modules

- Module General
  - HTTP Basic, HTTP proxies, and Developer Tools it’s **VERY** important you do all four
  - Those modules teach you how to use the tools!
- Module (A1) Broken Access Control
  - All
- Module (A7) Identity and Auth Failure
  - Authentication Bypasses
  - Insecure Login

Report

- You can do the labs in pairs, or alone, depending on your preference
- Discuss the 6 complete modules (4 modules A1, 2 modules A7)
  - What did you learn? Any suggestions about how you can avoid these kind of hacks?
- Attach a couple of screenshots that show what you have done
  - Hackers take “trophy pictures” all the time, vanity is the keyword! ;-)
- Strict deadline for handing in the report
  - ***May 12th 23:59***

What is expected from you

- First, that you learn the basics of ZAP
  - Here you can find a video tutorial about linking ZAP to your browser, which complements the instructions found in WebGoat
    https://www.youtube.com/watch?v=MncS-Mfwm-8&list=PLrHVSJmDPvlqxCfBhPuksHdpViPyeZTsF&index=9&t=0s&app=desktop
- Second, that you try hard by yourself to get through all modules
- If you need help with your modules, refer to
  - https://hackmd.io/@DaLaw2/ByD70wAM2
  - https://www.youtube.com/playlist?list=PLrHVSJmDPvlqxCfBhPuksHdpViPyeZTsF

How you should do this lab

- Let’s face it, you mindlessly mirror the steps in the links
  - But you wouldn’t learn that much
- First, try as hard as you can to do the lab by yourself
  - If you’re stuck, check the step on the channel
  - Then try to proceed by yourself from there
  - Rinse and repeat